REMARKS

The Office Action dated July 6, 2007 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 6, 7, 9, 10, 16, 17, 20, 22, 33 and 35 are amended to more particularly point out and distinctly claim the subject matter of the present invention. Support for the amendments is found at least in page 9 of the present specification. Entry of the amendments is respectfully requested because they place the application into condition for allowance, do not raise new issues that require further search and/or consideration, and do not contain new matter. Claims 1-48 are respectfully submitted for consideration.

The Office Action rejected claims 2, 20, 28-30, 32, 33, 36-41 and 45-47 under 35 U.S.C. 112, second paragraph for being indefinite. Specifically regarding claims 20 and 33, the Office Action asserted that the phrase "or other similar" renders these claims to be indefinite. Applicants respectfully submit that claims 20 and 33 are amended to delete this phrase, and to insert the term "comprising".

Further, regarding claim 2, the Office Action asserted that the phrase "convey the results of the scanning process" lacks proper antecedent basis. Applicants respectfully submit that claim 2 is amended to provide proper antecedent basis for all of the recited features.

Applicants respectfully submit that claims 2, 20, 28-30, 32, 33, 36-41 and 45-47 particularly point out and distinctly claim the subject matter of the present invention.

Accordingly, withdrawal of the rejection under 35 U.S.C. 112, second paragraph is respectfully requested.

The Office Action rejected claims 1-5, 8-15, 19, 21, 22-26, 29, 31, 32, 34, 35-38, 42-44, 46 and 48 under 35 U.S.C. 102(e) as being anticipated by US Patent No. 7,058,970 to Shaw. Applicants respectfully submit that Shaw fails to disclose or suggest all of the features recited in any of the pending claims.

Claim 1, from which claims 2-8 depend, is directed to an apparatus for verifying the security integrity of remote network devices. A proxy device configured to receive a request for network services by at least one remote network device. A security integrity scanning operation is performed on the requesting remote network device. The security scanning operation is performed least one of before and after the remote network device signs on to the proxy device. An authorization processing unit and access control rules unit configured to determine if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

Claim 9, from which claims 10-21 depend, is directed to a system for verifying security integrity of remote network devices. At least one remote network device configured to accesses a network via a network connection to make a request for one or more network resident services. A gateway device configured to receive the request for services and perform a security integrity scanning operation on the remote network device prior to allowing access to the requested network services. The security scanning operation is performed at least one of before and after the remote network device signs on

to the gateway device. An authentication server verifies user authentication credentials of users of remote network devices that access the network. At least one network server provides requested network services to at least one remote network device accessing the network through the gateway device.

Claim 22, from which claims 23-43 depend is directed to a method for verifying security integrity of remote network devices. At least one variable used as a vehicle is defined to convey results of a scanning process. Verification software is downloaded via a network connection to the remote network device that performs scanning process and reports result used in scanning script, including at least one variable. At least one scanning operation is performed on the remote network device to verify the security integrity of the remote device. The scanning operation is performed at least one of before and after the remote device signs on to a gateway device which is configured to perform the at least one scanning operation. The results of the scanning operation are obtained for purposes of determining whether or not the remote network device is authorized to access the requested network services.

Claim 35, from which claims 36-48 depend, is directed to a method for assessing the integrity of remote network devices for purposes of regulating access to network services via a network gateway. At least one access control policy is defined for accessing network services. The access control policy depends, at least in part, on the results of an integrity scan performed on the remote network device. Verification software is downloaded that an administrator can specify what scan scripts are to used

under what conditions to the remote network device. An integrity scan is performed on the remote network device and conveying at least one result of the scan to a gateway device. The integrity scan is performed at least one of before and after the remote device signs on to the gateway device. Access is regulated by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

According to certain embodiments of the presently claimed invention, a gateway is configured to prevent a user from accessing the gateway sign-on page from a network device that already may have been compromised by a hacker. Thus, the user will also avoid entering passwords on insecure remote devices. See for example, page 9 line 18-page 10 line 15 of the present specification. Applicants respectfully submit that each of the above claims recites features that are neither disclosed nor suggested in Shaw.

Shaw is directed to a network security authority system that provides on-connect scan and delivery in a virtual lobby to enforce security requirements for a network. One embodiment of a network security authority includes two firewalls around a virtual lobby. The virtual lobby includes at least one computing system and one or more software components capable of causing the computing system(s) to operate to protect the network. The virtual lobby is utilized to ensure that any client that connects into the network has certain types of protection, such as proper virus protection software in order to avoid risks like spreading viruses.

Applicants respectfully submit that Shaw fails to disclose or suggest at least the feature of "a proxy device for receiving a request for network services by at least one remote network device and performing a security integrity scanning operation on the requesting remote network device, wherein the scan is performed at least one of before and after the remote device signs on to the gateway device," and "determining if the remote network device is authorized to access the requested network services based on the results of the security scanning operation", as recited in clam 1 and similarly recited in claims 9, 22, and 35.

As discussed above, present claims 1, 9, 22, and 35 recite the feature that the security scan is performed at least one of before and after the remote device signs on to the gateway device. Applicants respectfully submit that Shaw fails to disclose or suggest this feature. As previously discussed, Shaw merely describes that the gateway sign on page can be accessed from a remote device that has already been compromised by an attacker. Thus, in the event that the correct enterprise passwords are entered, access will be gained by an insecure remote device.

In the "Response to Arguments" section, the Office Action asserted that the features upon which applicants relies are not recited in the present claims. Applicants respectfully submit that each of the claimed features discussed above, are recited in the present pending claims.

Applicants further submit that the Shaw fails to even suggest the above discussed features. Therefore, Shaw fails to contemplate the advantages of the presently claimed invention.

Applicants submit that because claims 2-5, 8, 10-15, 19, 21, 23-26, 29, 31, 32, 34, 36-38, 42-44, 46 and 48 depend from claims 1, 9, 22 and 35, these claims are allowable at least for the same reasons as claims 1, 9, 22 and 35, as well as for the additional features recited in these dependent claims.

Based at least on the above, Applicants respectfully submit that Shaw fails to disclose or suggest all of the features of claims 1-5, 8-15, 19, 21, 23-26, 29, 31, 32, 34-38, 42-44, 46 and 48. Accordingly, withdrawal of the rejection under 35 U.S.C. 102(e) is respectfully requested.

The Office Action rejected claims 6, 7, 16-18, 27, 28, 30, 40, 41 and 45 under 35 U.S.C. 103(a) as being obvious over Shaw, in view of US Patent No. 6,728,886 to Ji et al. (Ji). The Office Action took the position that Shaw disclosed most of the features of these claims except a signed applet, executing the script allowed to access the remote device for the purposes of executing programs as well as searching and reading specific data filed that reside on the remote network device. The Office Action asserted that Ji disclosed these features. Applicants submit that the cited references, taken individually or in combination, fail to disclose or suggest all of the features of any of the above claims. Specifically, Shaw is deficient at least for the same reasons discussed above regarding claims 1, 9, 22, and 35, and Ji fails to cure these deficiencies.

As discussed in previous correspondence, Ji is directed to detecting viruses that may be transferred between a distributed computer network, such as the Internet, and a host computer. A host computer performs its own virus scanning on data, using executables code downloaded to its browser upon a request for data from the Internet, such as an HTTP request. Code is downloaded to the host computer, and is configured to create a virus scan module on the host computer upon such a request. The module is used to detect viruses in data transferred between the host computer and the Internet. However, Applicants respectfully submits that Ji fails to cure the significant deficiencies of Shaw discussed above.

Based at least on the above, Applicants submit that the cited references fail to disclose or suggest all of the features of claims 6, 7, 16-18, 27, 28, 30, 40, 41 and 45. Accordingly, withdrawal of the rejection under 35 U.S.C. 103(a) is respectfully requested.

The Office Action rejected claims 6, 7, 16, 17, 18, 27, 28, 30, 40, 41 and 45 under 35 U.S.C. 103(a) as being obvious over Shaw, in view of US Patent Publication No. 2003/0177392 to Hiltgen. The Office Action took the position that Shaw disclosed all of the features of these claims except SSL to protect data communication between the remote device and the gateway device, and establishing communication between the remote device and the gateway using WAP. The Office Action relied on Hiltgen to disclose these features. Applicants respectfully submit that the cited references, taken individually or in combination, fail to disclose or suggest all of the features recited in any

of the pending claims. Specifically, Shaw is deficient at least for the reasons discussed above, and Hiltgen fails to cure these deficiencies.

Hiltgen is directed to secure user authentication over a network. The client uses has access to the network via a card reader for eh smart card. A first authentication key is used to start an encryption process. A second authentication key is used to perform a second authentication step. However, Applicants respectfully submit that Hiltgen fails to disclose or suggest at least the features of "a proxy device for receiving a request for network services by at least one remote network device, performing a security integrity scanning operation on the requesting remote network device, wherein the scan is performed at least one of before and after the remote device signs on to the gateway device," and "determining if the remote network device is authorized to access the requested network services based on the results of the security scanning operation." Thus, Hiltgen fails to cure the significant deficiencies of Shaw.

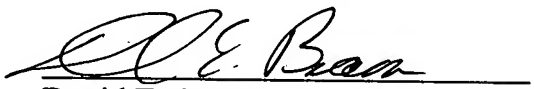
Based at least on the above, Applicants submit that the cited references fail to disclose or suggest all of the features of claims 6, 7, 16-18, 27, 28, 30, 40, 41 and 45. Accordingly, withdrawal of the rejection under 35 U.S.C. 103(a) is respectfully requested.

Applicants submit that each of claims 1-48 recite features that are neither disclosed nor suggested in any of the cited references. Accordingly, it is respectfully requested that each of claims 1-48 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DEB:dc:jkm